

# Cayley graphs of diameter two with order greater than 0.684 of the Moore bound for any degree

Marcel Abas<sup>a,\*</sup>

<sup>a</sup>*Institute of Applied Informatics, Automation and Mathematics,  
Faculty of Materials Science and Technology in Trnava,  
Slovak University of Technology in Bratislava, Trnava, Slovakia*

---

## Abstract

It is known that the number of vertices of a graph of diameter two cannot exceed  $d^2 + 1$ . In this contribution we give a new lower bound for orders of Cayley graphs of diameter two in the form  $C(d, 2) > 0.684d^2$  valid for all degrees  $d \geq 360756$ . The result is a significant improvement of currently known results on the orders of Cayley graphs of diameter two.

*Keywords:* Degree; Diameter; Moore bound; Cayley graph, Networks.

---

## 1. Introduction

Networks (optical, interconnection, etc.) are usually modeled by graphs (digraphs), where nodes of the network are represented by vertices and communication lines are represented by undirected (directed) edges. Therefore the designing of networks is closely linked to constructing (di)graphs with some preassigned properties. Obviously, the basic limitation on any network is the number of communication lines connected to a node and the maximum communication delay. These two parameters correspond to the degree (in/out degree) of the corresponding vertex and to the diameter of the (di)graph, respectively.

From now on, by graph we will mean a graph, which is finite, connected and simple (i.e. undirected, without loops and multiple edges). In graph theory, the problem to find the largest order  $n(d, k)$  of a graph with given maximum degree  $d$  and diameter  $k$  is known as *degree-diameter* problem. The well known upper bound on the number  $n(d, k)$  is *Moore bound* which gives  $n(d, k) \leq 1 + d + d(d-1) + d(d-1)^2 + \dots + d(d-1)^{k-1}$  for every  $d, k \geq 1$ . The graphs satisfying the Moore bound are known as *Moore graphs*. Except  $k = 1$  or  $d \leq 2$  there are only few graphs achieving the Moore bound. For  $k = 1, d \geq 1$  we have  $n(d, 1) = d + 1$  (achieved by complete graphs  $K_{d+1}$ ) and for  $d = 2, k \geq 1$  we have  $n(2, d) = 2d + 1$  (odd-length cycles  $C_{2k+1}$ ). In [8] Hoffman and Singleton

---

\*Corresponding author

Email address: abas@stuba.sk (Marcel Abas)

proved that for  $k = 2$  there exists Moore graph only for degrees  $d \in \{2, 3, 7\}$  and (maybe) for  $d = 57$ . For the first three values of  $d$  the corresponding Moore graph is unique. It is the 5-cycle  $C_5$  for  $d = 2$ , Petersen graph for  $d = 3$  and Hoffman–Singleton graph for  $d = 7$ . Until now it is not known yet if a Moore graph of degree  $d = 57$  and diameter  $k = 2$  on 3250 vertices does exist. However, it was shown by Cameron [4] that if there is a Moore graph for  $d = 57$  and  $k = 2$ , the graph is not vertex-transitive, in contrast to the fact that the other Moore graphs are vertex-transitive. In addition, Mačaj and Širáň proved [9] that the order of the automorphism group of the (hypothetical) Moore graph is at most 375. It was shown by Damerell [6] that for  $d \geq 3$  and  $k \geq 3$  there is no Moore graph. That is for other combinations of degrees and diameters there are no other Moore graphs. For a summary on the history and development on this topic we refer to survey paper of Miller and Širáň [11].

The Moore bound for diameter two is  $n(d, 2) \leq d^2 + 1$ , and it was shown by Erdős, Fajtlowicz and Hoffman [7] that for  $d \geq 4$ ,  $d \neq 7$  and  $d \neq 57$ , the bound is  $n(d, 2) \leq d^2 - 1$ . An explicit lower bound  $n(d, 2) \geq d^2 - d + i$  is given by Brown’s graphs [3] for all  $d$  such that  $d - 1$  is a prime power and  $i = 2$  for  $d - 1$  even and  $i = 1$  for  $d - 1$  odd. A modification of Brown’s graphs constructed by Širáň, Šiagiová and Ždímalová [15] gives the lower bound  $n(d, 2) \geq d^2 - 2d^{1.525}$  for all sufficiently large  $d$ . Since neither the Brown’s graphs nor their modification are vertex-transitive, it is a natural question to ask what is the maximum number of vertices of a vertex-transitive graph or a Cayley graph of diameter two and degree  $d$ . These numbers we will denote by  $v(d, 2)$  and  $C(d, 2)$ , respectively. As the Cayley graphs are vertex-transitive, we have  $n(d, 2) \geq v(d, 2) \geq C(d, 2)$  for each degree  $d$ .

Currently, the best known construction of vertex-transitive graphs are McKay–Miller–Širáň graphs [10] which give  $v(d, 2) \geq \frac{8}{9}(d + \frac{1}{2})^2$ , for degrees  $d = \frac{1}{2}(3q - 1)$  such that  $q \equiv 1 \pmod{4}$  is a prime power. In the same paper the authors have shown that all these graphs are non-Cayley.

For Cayley graphs we have the following results. Until recently, the best known lower bound valid for all degrees  $d$  there was a folklore bound giving  $C(d, 2) \geq \frac{1}{4}d^2 + d + 1$  for even  $d$  and  $\frac{1}{4}d^2 + d + \frac{3}{4}$  for odd  $d$ . Šiagiová and Širáň in [13] constructed Cayley graphs of diameter two and of order  $\frac{1}{2}(d + 1)^2$  for all degrees  $d = 2q - 1$  where  $q$  is an odd prime power and the same authors gave a construction [14] of Cayley graphs of diameter two and of order  $d^2 - O(d^{\frac{1}{2}})$  for an infinite set of degrees  $d$  of a very special type. Very recently Abas [1, 2] has shown that for all degrees  $d \geq 4$  we have  $C(d, 2) \geq \frac{1}{2}d^2$ .

In this contribution we show that for every degree  $d = 17n - 1$ ,  $n \geq 1$ , such that  $n \equiv 1 \pmod{10}$  is a prime, there is a Cayley graph of diameter two and of order  $\frac{200}{289}(d + 1)^2$ . Using explicit estimates for the distribution of primes in arithmetic progressions we show that for every  $d \geq 360756$  there is a Cayley graph of diameter two and of order greater than  $0.684d^2$ . This is a significant improvement of the known results valid for all degrees. In addition, we show that our construction provides infinitely many currently largest known Cayley graphs of diameter two.

## 2. Preliminaries

Let  $\Gamma$  be a finite group and let  $X \subset \Gamma$  be a unit-free, inverse-closed generating set for  $\Gamma$ . That is,  $1_\Gamma \notin X$ ,  $X = X^{-1}$  and  $\Gamma = \langle X \rangle$ . The Cayley graph  $G = \text{Cay}(\Gamma, X)$  for the *underlying* group  $\Gamma$  and the *generating* set  $X$  is a graph with vertex set  $V(G) = \Gamma$  and edge set  $E(G) = \{\{g, h\} | g \in \Gamma, g^{-1}h \in X\}$ . Since the set  $X$  is inverse closed,  $g^{-1}h \in X$  imply  $h^{-1}g \in X$  and therefore our Cayley graphs are undirected. Note that the mapping  $\varphi_h : V(G) \rightarrow V(G)$  defined by  $\varphi_h(g) = hg$ ,  $g \in V(G) = \Gamma$ , is a graph automorphism for each  $h \in \Gamma$ . It follows that every Cayley graph is vertex-transitive.

Throughout this paper, we will denote by  $\mathbb{Z}_n$  the cyclic group of order  $n$ , by  $\mathbb{Z}_n^2 = \mathbb{Z}_n \times \mathbb{Z}_n$  the direct product of  $\mathbb{Z}_n$  with itself, and by  $\mathbb{Z}_n^\times$  the multiplicative group of units modulo  $n$ . We will write the cyclic group  $\mathbb{Z}_n$  as an additive group with elements  $0, 1, \dots, n-1$ , with identity element 0 and with  $-x$  as the inverse element to  $x$ . The elements of  $\mathbb{Z}_n^2$  will be written in the form  $(x, y)$ ,  $x, y \in \mathbb{Z}_n$ , and the product of two elements of  $\mathbb{Z}_n^2$  will be  $(x_1, y_1) \cdot (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$ .

Let  $\alpha \in \mathbb{Z}_n^\times$  and let  $A : \mathbb{Z}_n^2 \rightarrow \mathbb{Z}_n^2$  be an automorphism of  $\mathbb{Z}_n^2$  given by  $A : (x, y) \rightarrow (\alpha x, y)$ . Clearly, if the order of  $\alpha$  in  $\mathbb{Z}_n^\times$  is  $k$  then  $k$  is the order of the automorphism  $A$ . Let  $B : \mathbb{Z}_n^2 \rightarrow \mathbb{Z}_n^2$  be another automorphism of  $\mathbb{Z}_n^2$  given by  $B : (x, y) \rightarrow (y, x)$  and let  $\Delta = \Delta(n, \alpha)$  be the group generated by  $A$  and  $B$ . That is,  $\Delta(n, \alpha) = \langle A, B \rangle$ . One can see that if the order of  $\alpha \in \mathbb{Z}_n^\times$  is the same as the order of  $\alpha' \in \mathbb{Z}_{n'}^\times$ , say  $k$ , then the groups  $\Delta(n, \alpha)$  and  $\Delta(n', \alpha')$  are isomorphic. Therefore the structure of  $\Delta(n, \alpha)$  depends only on the order  $k$  of  $\alpha$  in  $\mathbb{Z}_n^\times$  and we will write it simply as  $\Delta_k$ . The group  $\Delta_k$  has a presentation  $\Delta_k = \langle A, B | A^k = B^2 = (AB)^2(A^{-1}B)^2 = 1_{\Delta_k} \rangle$ .

Now suppose we have a group with presentation  $\langle a, b, c | a^k = b^k = c^2, ba = ab, cb = ac \rangle$ . One can see that this group is isomorphic to the group  $\Delta_k$  via the mapping  $A \rightarrow a, BAB \rightarrow b$  and  $B \rightarrow c$ . Elements of the group  $\langle a, b, c \rangle$  can be written in the form  $(x, y, i)$ , where  $x, y \in \mathbb{Z}_k$  and  $i \in \mathbb{Z}_2$ . Therefore the group  $\Delta_k$  is isomorphic to semidirect product of  $\mathbb{Z}_k^2$  with  $\mathbb{Z}_2$ , that is  $\Delta_k = \mathbb{Z}_k^2 \rtimes \mathbb{Z}_2$ , where the non-identity element of  $\mathbb{Z}_2$  interchanges the coordinates of elements of  $\mathbb{Z}_k^2$ . We will write the elements of  $\Delta_k$  as triples  $(x, y, i)$ , where  $x, y \in \{0, 1, \dots, k-1\}$  and  $i \in \{0, 1\}$ . The product of two elements of  $\Delta_k$  is given by  $(x_0, x_1, i) \cdot (y_0, y_1, j) = (x_0 + y_i, x_1 + y_{1-i}, i + j)$ , where the first two coordinates are taken modulo  $k$  and the last coordinate is taken modulo 2. The inverse element to  $(x_0, x_1, i)$  is  $(-x_i, -x_{1-i}, i)$ . Clearly, the order of the group  $\Delta_k$  is  $2k^2$ .

Let  $\alpha \in \mathbb{Z}_n^\times$  have order  $k$ . We will denote the semidirect product  $\mathbb{Z}_n^2 \rtimes_\alpha \Delta_k$  by the symbol  $\Gamma(n, \alpha)$  (obviously,  $\Gamma$  is uniquely determined by  $n$  and  $\alpha$ ). For the automorphisms  $a, b, c \in \Delta_k$  of  $\mathbb{Z}_n^2$  then we have:  $a : (x, y) \rightarrow (\alpha x, y)$ ,  $b : (x, y) \rightarrow (x, \alpha y)$  and  $c : (x, y) \rightarrow (y, x)$ . It is easy to see that the order of the group  $\Gamma(n, \alpha)$  is  $2n^2k^2$ . We will write the elements of  $\Gamma(n, \alpha)$  as quintuples  $(x_0, x_1; y_0, y_1, i)$ ,  $x_0, x_1 \in \mathbb{Z}_n$ ,  $y_0, y_1 \in \mathbb{Z}_k$ ,  $i \in \mathbb{Z}_2$ . Since the automorphism  $(y_0, y_1, i) \in \Delta_k$  maps an element  $(x_0, x_1)$  of  $\mathbb{Z}_n^2$  to the element  $(\alpha^{y_0}x_i, \alpha^{y_1}x_{1-i})$ , for the product of two elements of  $\Gamma(n, \alpha)$  we have  $(x_0, x_1; y_0, y_1, i) \cdot (x'_0, x'_1; y'_0, y'_1, i') = (x_0 + \alpha^{y_0}x'_i, x_1 + \alpha^{y_1}x'_{1-i}; y_0 + y'_i, y_1 + y'_{1-i}, i + i')$ ,

where the first two coordinates are taken modulo  $n$ , the second two are taken modulo  $k$  and the last coordinate is taken modulo 2.

In the following two lemmas we show that prime numbers of the form  $p \equiv 1 \pmod{10}$  have some special properties. We will need the lemmas in the proof of Theorem 1.

**Lemma 1.** *Let  $p = 10s + 1$ ,  $s \geq 1$ , be a prime number. Then there exists an integer  $\alpha$ ,  $1 < \alpha < p - 1$ , such that:*

- i)  $\alpha^{10} \equiv 1 \pmod{p}$ ,
- ii)  $\gcd(\alpha^i - 1, p) = 1$ ,  $2 \leq i \leq 5$ ,
- iii)  $\gcd(\alpha^i + 1, p) = 1$ ,  $i = 3, 4$ ,
- iv)  $\alpha^5 \equiv -1 \pmod{p}$ .

*Proof.* Let  $a$  be a primitive root of  $p$ . The multiplicative order of  $a$  modulo  $p$  is equal to  $\varphi(p) = 10s$  (note that  $\varphi(n)$  is the Euler's totient function - the number of positive integers less than or equal to  $n$  that are relatively prime to  $n$ ). Let  $\alpha = a^s$ . Since  $\alpha^2 = a^{2s} \not\equiv 1 \pmod{p}$ , or equivalently  $\gcd(\alpha^2 - 1, p) = 1$ , we have  $\alpha \not\equiv \pm 1 \pmod{p}$  and consequently  $1 < \alpha < p - 1$ . We claim that  $\alpha$  has the required properties i), ii), iii) and iv).

- i)  $\alpha^{10} \equiv 1 \pmod{p}$ : Clearly,  $\alpha^{10} = a^{10s} = a^{\varphi(p)} \equiv 1 \pmod{p}$ .
- ii)  $\gcd(\alpha^i - 1, p) = 1$ ,  $2 \leq i \leq 5$ : It follows immediately from the fact that  $\alpha$  is a power of a primitive root of  $p$ .
- iii)  $\gcd(\alpha^i + 1, p) = 1$ ,  $i = 3, 4$ : If  $\gcd(\alpha^i + 1, p) > 1$  then  $\alpha^i \equiv -1 \pmod{p}$  and consequently  $\alpha^{2i} \equiv 1 \pmod{p}$ , for  $2i = 6$  or  $8$ , which is a contradiction with the definition of  $\alpha$ .
- iv)  $\alpha^5 \equiv -1 \pmod{p}$ : From  $\alpha^{10} \equiv 1 \pmod{p}$  we have  $\alpha^{10} - 1 = (\alpha^5 + 1)(\alpha^5 - 1) \equiv 0 \pmod{p}$ . Since  $\alpha^5 \not\equiv 1 \pmod{p}$ , and  $p$  is a prime, it follows that  $\alpha^5 \equiv -1 \pmod{p}$ .  $\square$

**Lemma 2.** *Let  $p$  and  $\alpha$  be as in the previous lemma and let  $\Lambda = \Lambda_1 \cup \Lambda_2$ , where  $\Lambda_1 = \{\pm\alpha^i, \pm 2\alpha^i \mid 0 \leq i \leq 4\}$  and  $\Lambda_2 = \{\pm\alpha^i \pm \alpha^j \mid i, j = 0, 1, 2, 3, 4, i \neq j\}$ . Then every element of  $\Lambda$  is coprime with  $p$ .*

*Proof.*

- 1) Let  $\lambda \in \Lambda_1$ . Since  $2, -2$  and  $\alpha^i, -\alpha^i$  are coprimes with  $p$ , the result follows.
- 2) Let  $\lambda \in \Lambda_2$  and let  $j = 0$ . That is  $\lambda = \pm\alpha^i \pm 1$ . It follows from the previous lemma that  $\gcd(\lambda, p) = 1$ .
- 3) Let  $i, j > 0$  and let (without loss of generality)  $j \leq i$ . Then  $\lambda = \pm\alpha^i \pm \alpha^j = \alpha^j \cdot (\pm\alpha^{i'} \pm 1)$ , where  $0 \leq i' \leq 3$ . Since both factors of the product are coprime with  $p$ , the lemma is proven.  $\square$

We will use Corollary 2 of the following lemma in the proof of Theorem 1.

**Lemma 3.** *A mapping  $\varphi : \mathbb{Z}_n^2 \rightarrow \mathbb{Z}_n^2$  given by  $\varphi : (x, y) \rightarrow (a_1x + b_1y, a_2x + b_2y)$  is a group automorphism if and only if the determinant  $D = \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}$  is coprime with  $n$ .*

*Proof.* It immediately follows from the fact that the mapping  $\varphi : (x, y) \rightarrow (a_1x + b_1y, a_2x + b_2y)$  is an automorphism of  $\mathcal{Z}_n^2$  if and only if the matrix  $\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}$  is invertible over the ring of integers  $\mathcal{Z}/n\mathcal{Z}$ .  $\square$

So we have the following corollary:

**Corollary 1.** *System  $\begin{matrix} a_1x + b_1y = c_1 \\ a_2x + b_2y = c_2 \end{matrix}$  of linear equations over  $\mathcal{Z}_n$  has a unique solution in  $\mathcal{Z}_n$  if and only if the determinant  $D = \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}$  is coprime with  $n$ .*

**Corollary 2.** *Let  $\alpha \in \mathcal{Z}_n^\times$  has order  $k$ , let  $g_1(x) = (a_1x, b_1x; s_1)$ , let  $g_2(x) = (a_2x, b_2x; s_2)$  and let  $s = s_1 \cdot s_2$ ,  $a_1, a_2, b_1, b_2, x \in \mathcal{Z}_n$ ,  $s_1, s_2 \in \Delta_k$ . Let  $g_1(x) \cdot g_2(y) = (ax + by, cx + dy; s)$ , for some  $a, b, c, d \in \mathcal{Z}_n$ . If the determinant  $D = \begin{vmatrix} a & b \\ c & d \end{vmatrix}$  is coprime with  $n$  then for each  $(u, v) \in \mathcal{Z}_n^2$  there is exactly one element  $(x, y) \in \mathcal{Z}_n^2$  such that  $g_1(x) \cdot g_2(y) = (u, v; s)$ .*

*Proof.* It follows from Corollary 1.  $\square$

### 3. Results

For the rest of this paper,  $P$  will denote the set of all primes of the form  $p \equiv 1 \pmod{10}$ .

**Theorem 1.** *Let  $n \in P \cup \{1\}$  and let  $d = 17n - 1$ . Then there exists a Cayley graph of diameter two, degree  $d$  and of order  $\frac{200}{289}(d+1)^2$ .*

*Proof.* Let  $n = p > 1$  and  $\alpha$  be as in Lemma 1. Let  $\Gamma = \Gamma(n, \alpha) = \mathcal{Z}_n^2 \rtimes_\alpha \Delta_{10}$  and for  $x \in \mathcal{Z}_n$  we set  $a(x) = (x, x; 5, 0, 0)$ ,  $b(x) = (x, -x; 0, 0, 1)$ ,  $c(x) = (x, x; 1, 0, 1)$ ,  $d(x) = (x, 0; 5, 0, 1)$ ,  $e(x) = (x, \alpha^3x; 1, 3, 1)$ ,  $f(x) = (x, x; 1, 7, 1)$ ,  $g(x) = (0, x; 5, 2, 1)$ ,  $h(x) = (x, \alpha x; 3, 2, 0)$  and  $k(x) = (x, \alpha x; 4, 1, 0)$ . We can see that  $a^{-1}(x) = (x, -x; 5, 0, 0)$ ,  $b^{-1}(x) = (x, -x; 0, 0, 1)$ ,  $c^{-1}(x) = (-x, \alpha^4x; 0, 9, 1)$ ,  $d^{-1}(x) = (0, x; 0, 5, 1)$ ,  $e^{-1}(x) = (-x, \alpha^4x; 7, 9, 1)$ ,  $f^{-1}(x) = (-\alpha^3x, \alpha^4x; 3, 9, 1)$ ,  $g^{-1}(x) = (\alpha^3x, 0; 8, 5, 1)$ ,  $h^{-1}(x) = (\alpha^2x, \alpha^4x; 7, 8, 0)$  and  $k^{-1}(x) = (\alpha x, \alpha^4x; 6, 9, 0)$ .

Let  $X = \{a(x), a^{-1}(x), b(x), b^{-1}(x), c(x), c^{-1}(x), d(x), d^{-1}(x), e(x), e^{-1}(x), f(x), f^{-1}(x), g(x), g^{-1}(x), h(x), h^{-1}(x), k(x), k^{-1}(x) | x \in \mathcal{Z}_n\}$  and let  $G = \text{Cay}(\Gamma, X)$  be the Cayley graph for the underlying group  $\Gamma$  and the generating set  $X$ . Since  $b(x) = b^{-1}(x)$  for each  $x \in \mathcal{Z}_n$ , and  $a(x) = a^{-1}(x)$  exactly when  $x = 0$ , the set  $X$  has  $17n - 1$  elements. As the group  $\Gamma$  has order  $|\Gamma| = 2n^2 \cdot 10^2 = 200n^2$  and the degree of  $G$  is  $d = 17n - 1$ , the corresponding Cayley graph has order  $\frac{200}{289}(d+1)^2$ . Now let a set  $S \subset \Delta_{10}$  consists of elements  $(i, j, 0)$  such that  $i = 0, 0 \leq j \leq 5; 1 \leq i \leq 5, 0 \leq j \leq 10 - i; 6 \leq i \leq 8, 1 \leq j \leq 9 - i$  and of the elements  $(i, j, 1)$  such that  $i = 0, j = 0$  and  $1 \leq i \leq 9, 0 \leq j \leq 10 - i$ . We can see that  $S \cup S^{-1} = \Delta_{10}$ .

Since the generating set  $X$  is inverse-closed, to prove that  $G$  has diameter two, it is sufficient to show that every element of  $\Gamma$  of the form  $(x, y; s), x, y \in$

$\mathcal{Z}_n, s \in S$  can be generated as a product of two elements from  $X$ . For every  $s \in S$  we show that there is  $g_1(x), g_2(y) \in X$  (see Corollary 2) such that the determinant corresponding to the product  $g_1(x) \cdot g_2(y)$  is coprime with  $n$ .

For the product of  $a(x)$  and  $a(y)$  we have  $a(x) \cdot a(y) = (x, x; 5, 0, 0) \cdot (y, y; 5, 0, 0) = (x + \alpha^5 y, x + y; 0, 0, 0) = (x - y, x + y; 0, 0, 0)$ . We have to show that for any  $(u, v) \in \mathcal{Z}_n^2$  there is  $x, y \in \mathcal{Z}_n$  such that  $(x - y, x + y) = (u, v)$ . Since the determinant  $D = \begin{vmatrix} 1 & -1 \\ 1 & 1 \end{vmatrix} = 2$ , it is coprime with  $n$ , and therefore the system  $x - y = u$  and  $x + y = v$  has a (unique) solution for each  $(u, v) \in \mathcal{Z}_n^2$ . In the table below we can see how to generate the other elements of  $\Gamma$ .

	Product of generators	Determinant
1.	$a(x) \cdot a(x) = (x - y, x + y; 0, 0, 0)$	$\begin{vmatrix} 1 & -1 \\ 1 & 1 \end{vmatrix} = 2$
2.	$c(x) \cdot b(y) = (x - \alpha y, x + y; 1, 0, 0)$	$\begin{vmatrix} 1 & -\alpha \\ 1 & 1 \end{vmatrix} = \alpha + 1$
3.	$d^{-1}(x) \cdot g(y) = (y, x; 2, 0, 0)$	$\begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} = -1$
4.	$c^{-1}(x) \cdot e(y) = (-x + \alpha^3 y, \alpha^4 x - \alpha^4 y; 3, 0, 0)$	$\begin{vmatrix} -1 & \alpha^3 \\ \alpha^4 & -\alpha^4 \end{vmatrix} = \alpha^4 + \alpha^2$
5.	$d(x) \cdot c^{-1}(y) = (x - \alpha^4 y, -y; 4, 0, 0)$	$\begin{vmatrix} 1 & -\alpha^4 \\ 0 & -1 \end{vmatrix} = -1$
6.	$d(x) \cdot b(y) = (x + y, y; 5, 0, 0)$	$\begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix} = 1$
7.	$b(x) \cdot c(y) = (x + y, -x + y; 0, 1, 0)$	$\begin{vmatrix} 1 & 1 \\ -1 & 1 \end{vmatrix} = 2$
8.	$g(x) \cdot d^{-1}(y) = (-y, x; 0, 2, 0)$	$\begin{vmatrix} 0 & -1 \\ 1 & 0 \end{vmatrix} = 1$
9.	$c(x) \cdot f^{-1}(y) = (x - \alpha y, x - \alpha^3 y; 0, 3, 0)$	$\begin{vmatrix} 1 & -\alpha \\ 1 & -\alpha^3 \end{vmatrix} = -\alpha^3 + \alpha$
10.	$f(x) \cdot e^{-1}(y) = (x - y, x + \alpha^2 y; 0, 4, 0)$	$\begin{vmatrix} 1 & -1 \\ 1 & \alpha^2 \end{vmatrix} = \alpha^2 + 1$
11.	$b(x) \cdot d(y) = (x, -x + y; 0, 5, 0)$	$\begin{vmatrix} 1 & 0 \\ -1 & 1 \end{vmatrix} = 1$
12.	$c(x) \cdot c(y) = (x + \alpha y, x + y; 1, 1, 0)$	$\begin{vmatrix} 1 & \alpha \\ 1 & 1 \end{vmatrix} = 1 - \alpha$
13.	$f(x) \cdot d(y) = (x, x - \alpha^2 y; 1, 2, 0)$	$\begin{vmatrix} 1 & 0 \\ 1 & -\alpha^2 \end{vmatrix} = -\alpha^2$
14.	$e(x) \cdot b(y) = (x - \alpha y, \alpha^3 x + \alpha^3 y; 1, 3, 0)$	$\begin{vmatrix} 1 & -\alpha \\ \alpha^3 & \alpha^3 \end{vmatrix} = \alpha^4 + \alpha^3$
15.	$e(x) \cdot c(y) = (x + \alpha y, \alpha^3 x + \alpha^3 y; 1, 4, 0)$	$\begin{vmatrix} 1 & \alpha \\ \alpha^3 & \alpha^3 \end{vmatrix} = \alpha^3 - \alpha^4$
16.	$c(x) \cdot d(y) = (x, x + y; 1, 5, 0)$	$\begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix} = 1$
17.	$g^{-1}(x) \cdot e(y) = (\alpha^3 x + \alpha y, -y; 1, 6, 0)$	$\begin{vmatrix} \alpha^3 & \alpha \\ 0 & -1 \end{vmatrix} = -\alpha^3$
18.	$f(x) \cdot b(y) = (x - \alpha y, x - \alpha^2 y; 1, 7, 0)$	$\begin{vmatrix} 1 & -\alpha \\ 1 & -\alpha^2 \end{vmatrix} = \alpha - \alpha^2$
19.	$e(x) \cdot d(y) = (x, \alpha^3 x + \alpha^3 y; 1, 8, 0)$	$\begin{vmatrix} 1 & 0 \\ \alpha^3 & \alpha^3 \end{vmatrix} = \alpha^3$
20.	$a(x) \cdot k^{-1}(y) = (x - \alpha y, x + \alpha^4 y; 1, 9, 0)$	$\begin{vmatrix} 1 & -\alpha \\ 1 & \alpha^4 \end{vmatrix} = \alpha^4 + \alpha$
21.	$d(x) \cdot f(y) = (x - y, y; 2, 1, 0)$	$\begin{vmatrix} 1 & -1 \\ 0 & 1 \end{vmatrix} = 1$
22.	$f^{-1}(x) \cdot f^{-1}(y) = (-\alpha^3 x - \alpha^2 y, \alpha^4 x - \alpha^2 y; 2, 2, 0)$	$\begin{vmatrix} -\alpha^3 & -\alpha^2 \\ \alpha^4 & -\alpha^2 \end{vmatrix} = -\alpha - 1$

23.	$g(x) \cdot f(y) =$	$(-y, x + \alpha^2 y; 2, 3, 0)$	$\begin{vmatrix} 0 & -1 \\ 1 & \alpha^2 \end{vmatrix} = 1$
24.	$c^{-1}(x) \cdot g(y) =$	$(-x + y, \alpha^4 x; 2, 4, 0)$	$\begin{vmatrix} -1 & 1 \\ \alpha^4 & 0 \end{vmatrix} = -\alpha^4$
25.	$b(x) \cdot g(y) =$	$(x + y, -x; 2, 5, 0)$	$\begin{vmatrix} -1 & 1 \\ -1 & 0 \end{vmatrix} = 1$
26.	$f^{-1}(x) \cdot e^{-1}(y) =$	$(-\alpha^3 x - \alpha^2 y, \alpha^4 x + \alpha^4 y; 2, 6, 0)$	$\begin{vmatrix} -\alpha^3 & -\alpha^2 \\ \alpha^4 & \alpha^4 \end{vmatrix} = \alpha^2 - \alpha$
27.	$e^{-1}(x) \cdot g^{-1}(y) =$	$(-x, \alpha^4 x + \alpha^2 y; 2, 7, 0)$	$\begin{vmatrix} -1 & 0 \\ \alpha^4 & \alpha^2 \end{vmatrix} = -\alpha^2$
28.	$a(x) \cdot h^{-1}(y) =$	$(x - \alpha^2 y, x + \alpha^4 y; 2, 8, 0)$	$\begin{vmatrix} 1 & -\alpha^2 \\ 1 & \alpha^4 \end{vmatrix} = \alpha^4 + \alpha^2$
29.	$b(x) \cdot e(y) =$	$(x + \alpha^3 y, -x + y; 3, 1, 0)$	$\begin{vmatrix} -1 & \alpha^3 \\ -1 & 1 \end{vmatrix} = \alpha^3 + 1$
30.	$f(x) \cdot g(y) =$	$(x + \alpha y, x; 3, 2, 0)$	$\begin{vmatrix} 1 & \alpha \\ 1 & 0 \end{vmatrix} = -\alpha$
31.	$g^{-1}(x) \cdot g^{-1}(y) =$	$(\alpha^3 x, -\alpha^3 y; 3, 3, 0)$	$\begin{vmatrix} \alpha^3 & 0 \\ 0 & -\alpha^3 \end{vmatrix} = \alpha$
32.	$f^{-1}(x) \cdot d(y) =$	$(-\alpha^3 x, \alpha^4 x - \alpha^4 y; 3, 4, 0)$	$\begin{vmatrix} -\alpha^3 & 0 \\ \alpha^4 & -\alpha^4 \end{vmatrix} = -\alpha^2$
33.	$c(x) \cdot g(y) =$	$(x + \alpha y, x; 3, 5, 0)$	$\begin{vmatrix} 1 & \alpha \\ 1 & 0 \end{vmatrix} = -\alpha$
34.	$d^{-1}(x) \cdot e(y) =$	$(\alpha^3 y, x - y; 3, 6, 0)$	$\begin{vmatrix} 0 & \alpha^3 \\ 1 & -1 \end{vmatrix} = -\alpha^3$
35.	$h^{-1}(x) \cdot k^{-1}(y) =$	$(\alpha^2 x - \alpha^3 y, \alpha^4 x + \alpha^2 y; 3, 7, 0)$	$\begin{vmatrix} \alpha^2 & -\alpha^3 \\ \alpha^4 & \alpha^2 \end{vmatrix} = \alpha^4 - \alpha^2$
36.	$c(x) \cdot e(y) =$	$(x + \alpha^4 y, x + y; 4, 1, 0)$	$\begin{vmatrix} 1 & \alpha^4 \\ 1 & 1 \end{vmatrix} = 1 - \alpha^4$
37.	$g(x) \cdot c^{-1}(y) =$	$(-\alpha^4 y, x - \alpha^2 y; 4, 2, 0)$	$\begin{vmatrix} 0 & -\alpha^4 \\ 1 & -\alpha^2 \end{vmatrix} = \alpha^4$
38.	$d(x) \cdot f^{-1}(y) =$	$(x - \alpha^4 y, -\alpha^3 y; 4, 3, 0)$	$\begin{vmatrix} 1 & -\alpha^4 \\ 0 & -\alpha^3 \end{vmatrix} = -\alpha^3$
39.	$e(x) \cdot e(y) =$	$(x + \alpha^4 y, \alpha^3 x + \alpha^3 y; 4, 4, 0)$	$\begin{vmatrix} 1 & \alpha^4 \\ \alpha^3 & \alpha^3 \end{vmatrix} = \alpha^3 + \alpha^2$
40.	$g(x) \cdot f^{-1}(y) =$	$(-\alpha^4 y, x + y; 4, 5, 0)$	$\begin{vmatrix} 0 & -\alpha^4 \\ 1 & 1 \end{vmatrix} = \alpha^4$
41.	$h^{-1}(x) \cdot h^{-1}(y) =$	$(\alpha^2 x - \alpha^4 y, \alpha^4 x + \alpha^2 y; 4, 6, 0)$	$\begin{vmatrix} \alpha^2 & -\alpha^4 \\ \alpha^4 & \alpha^2 \end{vmatrix} = \alpha^4 - \alpha^3$
42.	$d(x) \cdot c(y) =$	$(x + y, -y; 5, 1, 0)$	$\begin{vmatrix} 1 & -1 \\ 0 & -1 \end{vmatrix} = -1$
43.	$g(x) \cdot b(y) =$	$(y, x + \alpha^2 y; 5, 2, 0)$	$\begin{vmatrix} 0 & 1 \\ 1 & \alpha^2 \end{vmatrix} = -1$
44.	$g(x) \cdot c(y) =$	$(-y, x + \alpha^2 y; 5, 3, 0)$	$\begin{vmatrix} 0 & -1 \\ 1 & \alpha^2 \end{vmatrix} = 1$
45.	$f^{-1}(x) \cdot g(y) =$	$(-\alpha^3 x + \alpha^3 y, \alpha^4 x; 5, 4, 0)$	$\begin{vmatrix} -\alpha^3 & \alpha^3 \\ \alpha^4 & 0 \end{vmatrix} = \alpha^2$
46.	$d(x) \cdot d(y) =$	$(x, -y; 5, 5, 0)$	$\begin{vmatrix} 1 & 0 \\ 0 & -1 \end{vmatrix} = -1$
47.	$e(x) \cdot g^{-1}(y) =$	$(x, \alpha^3 x - \alpha y; 6, 1, 0)$	$\begin{vmatrix} 1 & 0 \\ \alpha^3 & -\alpha \end{vmatrix} = -\alpha$
48.	$e^{-1}(x) \cdot f^{-1}(y) =$	$(-x + \alpha y, \alpha^4 x - \alpha^2 y; 6, 2, 0)$	$\begin{vmatrix} -1 & \alpha \\ \alpha^4 & -\alpha^2 \end{vmatrix} = \alpha^2 + 1$
49.	$e(x) \cdot d^{-1}(y) =$	$(x + \alpha y, \alpha^3 x; 6, 3, 0)$	$\begin{vmatrix} 1 & \alpha \\ \alpha^3 & 0 \end{vmatrix} = -\alpha^4$
50.	$b(x) \cdot f(y) =$	$(x + y, -x + y; 7, 1, 0)$	$\begin{vmatrix} -1 & 1 \\ -1 & 1 \end{vmatrix} = 2$
51.	$g^{-1}(x) \cdot e^{-1}(y) =$	$(\alpha^3 x + \alpha^2 y, y; 7, 2, 0)$	$\begin{vmatrix} \alpha^3 & \alpha^2 \\ 0 & 1 \end{vmatrix} = \alpha^3$

52.	$c(x) \cdot f(y) =$	$(x + \alpha y, x + y; 8, 1, 0)$	$\begin{vmatrix} 1 & \alpha \\ 1 & 1 \end{vmatrix} = 1 - \alpha$
53.	$a(x) \cdot d(y) =$	$(x - y, x; 0, 0, 1)$	$\begin{vmatrix} 1 & -1 \\ 1 & 0 \end{vmatrix} = 1$
54.	$k(x) \cdot e^{-1}(y) =$	$(x - \alpha^4 y, \alpha x - y; 1, 0, 1)$	$\begin{vmatrix} 1 & -\alpha^4 \\ \alpha & -1 \end{vmatrix} = -2$
55.	$h^{-1}(x) \cdot g(y) =$	$(\alpha^2 x, \alpha^4 x - \alpha^3 y; 2, 0, 1)$	$\begin{vmatrix} \alpha^2 & 0 \\ \alpha^4 & -\alpha^3 \end{vmatrix} = 1$
56.	$f(x) \cdot h(y) =$	$(x + \alpha^2 y, x - \alpha^2 y; 3, 0, 1)$	$\begin{vmatrix} 1 & \alpha^2 \\ 1 & -\alpha^2 \end{vmatrix} = -2\alpha^2$
57.	$k(x) \cdot c^{-1}(y) =$	$(x - \alpha^3 y, \alpha x - \alpha y; 4, 0, 1)$	$\begin{vmatrix} 1 & -\alpha^3 \\ \alpha & -\alpha \end{vmatrix} = \alpha^4 - \alpha$
58.	$a^{-1}(x) \cdot b(y) =$	$(x - y, -x - y; 5, 0, 1)$	$\begin{vmatrix} 1 & -1 \\ -1 & -1 \end{vmatrix} = -2$
59.	$a(x) \cdot c(y) =$	$(x - y, x + y; 6, 0, 1)$	$\begin{vmatrix} 1 & -1 \\ 1 & 1 \end{vmatrix} = 2$
60.	$k(x) \cdot f^{-1}(y) =$	$(x + \alpha^2 y, \alpha x - y; 7, 0, 1)$	$\begin{vmatrix} 1 & \alpha^2 \\ \alpha & -1 \end{vmatrix} = -\alpha^3 - 1$
61.	$g^{-1}(x) \cdot a(y) =$	$(\alpha^3 x - \alpha^3 y, -y; 8, 0, 1)$	$\begin{vmatrix} \alpha^3 & -\alpha^3 \\ 0 & -1 \end{vmatrix} = -\alpha^3$
62.	$e(x) \cdot h^{-1}(y) =$	$(x - y, \alpha^3 x - y; 9, 0, 1)$	$\begin{vmatrix} 1 & -1 \\ \alpha^3 & -1 \end{vmatrix} = \alpha^3 - 1$
63.	$k^{-1}(x) \cdot g(y) =$	$(\alpha x, \alpha^4 x - \alpha^4 y; 1, 1, 1)$	$\begin{vmatrix} \alpha & 0 \\ \alpha^4 & -\alpha^4 \end{vmatrix} = 1$
64.	$f(x) \cdot a(y) =$	$(x + \alpha y, x - \alpha^2 y; 1, 2, 1)$	$\begin{vmatrix} 1 & \alpha \\ 1 & -\alpha^2 \end{vmatrix} = -\alpha^2 - \alpha$
65.	$c^{-1}(x) \cdot k(y) =$	$(-x + \alpha y, \alpha^4 x - \alpha^4 y; 1, 3, 1)$	$\begin{vmatrix} -1 & \alpha \\ \alpha^4 & -\alpha^4 \end{vmatrix} = \alpha^4 + 1$
66.	$b(x) \cdot k(y) =$	$(x + \alpha y, -x + y; 1, 4, 1)$	$\begin{vmatrix} 1 & \alpha \\ -1 & 1 \end{vmatrix} = \alpha + 1$
67.	$c(x) \cdot a(y) =$	$(x + \alpha y, x + y; 1, 5, 1)$	$\begin{vmatrix} 1 & \alpha \\ 1 & 1 \end{vmatrix} = 1 - \alpha$
68.	$f^{-1}(x) \cdot h^{-1}(y) =$	$(-\alpha^3 x - \alpha^2 y, \alpha^4 x + \alpha y; 1, 6, 1)$	$\begin{vmatrix} -\alpha^3 & -\alpha^2 \\ \alpha^4 & \alpha \end{vmatrix} = -\alpha^4 + \alpha$
69.	$h(x) \cdot g^{-1}(y) =$	$(x - \alpha y, \alpha x; 1, 7, 1)$	$\begin{vmatrix} 1 & -\alpha \\ \alpha & 0 \end{vmatrix} = \alpha^2$
70.	$e(x) \cdot a(y) =$	$(x + \alpha^3 y, \alpha^3 x + \alpha^3 y; 1, 8, 1)$	$\begin{vmatrix} 1 & \alpha^3 \\ \alpha^3 & \alpha^3 \end{vmatrix} = \alpha^3 + \alpha$
71.	$k^{-1}(x) \cdot d(y) =$	$(\alpha x - \alpha y, \alpha^4 x; 1, 9, 1)$	$\begin{vmatrix} \alpha & -\alpha \\ \alpha^4 & 0 \end{vmatrix} = 1$
72.	$f(x) \cdot k(y) =$	$(x + \alpha^2 y, x - \alpha^2 y; 2, 1, 1)$	$\begin{vmatrix} 1 & \alpha^2 \\ 1 & -\alpha^2 \end{vmatrix} = -2\alpha^2$
73.	$c^{-1}(x) \cdot h(y) =$	$(-x + \alpha y, \alpha^4 x - \alpha^4 y; 2, 2, 1)$	$\begin{vmatrix} -1 & \alpha \\ \alpha^4 & -\alpha^4 \end{vmatrix} = \alpha^4 + 1$
74.	$b(x) \cdot h(y) =$	$(x + \alpha y, -x + y; 2, 3, 1)$	$\begin{vmatrix} 1 & \alpha \\ -1 & 1 \end{vmatrix} = \alpha + 1$
75.	$c(x) \cdot k(y) =$	$(x + \alpha^2 y, x + y; 2, 4, 1)$	$\begin{vmatrix} 1 & \alpha^2 \\ 1 & 1 \end{vmatrix} = 1 - \alpha^2$
76.	$f^{-1}(x) \cdot k^{-1}(y) =$	$(-\alpha^3 x - \alpha^2 y, \alpha^4 x + y; 2, 5, 1)$	$\begin{vmatrix} -\alpha^3 & -\alpha^2 \\ \alpha^4 & 1 \end{vmatrix} = -\alpha^3 - \alpha$
77.	$k(x) \cdot g^{-1}(y) =$	$(x - \alpha^2 y, \alpha x; 2, 6, 1)$	$\begin{vmatrix} 1 & -\alpha^2 \\ \alpha & 0 \end{vmatrix} = \alpha^3$
78.	$e(x) \cdot k(y) =$	$(x + \alpha^2 y, \alpha^3 x + \alpha^3 y; 2, 7, 1)$	$\begin{vmatrix} 1 & \alpha^2 \\ \alpha^3 & \alpha^3 \end{vmatrix} = \alpha^3 + 1$
79.	$h^{-1}(x) \cdot d(y) =$	$(\alpha^2 x - \alpha^2 y, \alpha^4 x; 2, 8, 1)$	$\begin{vmatrix} \alpha^2 & -\alpha^2 \\ \alpha^4 & 0 \end{vmatrix} = -\alpha$
80.	$h(x) \cdot c^{-1}(y) =$	$(x - \alpha^3 y, \alpha x - y; 3, 1, 1)$	$\begin{vmatrix} 1 & -\alpha^3 \\ \alpha & -1 \end{vmatrix} = \alpha^4 - 1$



81.	$h(x) \cdot b(y) = (x + \alpha^3 y, \alpha x - \alpha^2 y; 3, 2, 1)$	$\begin{vmatrix} 1 & \alpha^3 \\ \alpha & -\alpha^2 \end{vmatrix} = -\alpha^4 - \alpha^2$
82.	$c(x) \cdot h(y) = (x + \alpha^2 y, x + y; 3, 3, 1)$	$\begin{vmatrix} 1 & \alpha^2 \\ 1 & 1 \end{vmatrix} = 1 - \alpha^2$
83.	$f^{-1}(x) \cdot a^{-1}(y) = (-\alpha^3 x - \alpha^3 y, \alpha^4 x - \alpha^4 y; 3, 4, 1)$	$\begin{vmatrix} -\alpha^3 & -\alpha^3 \\ \alpha^4 & -\alpha^4 \end{vmatrix} = -2\alpha^2$
84.	$a(x) \cdot g^{-1}(y) = (x - \alpha^3 y, x; 3, 5, 1)$	$\begin{vmatrix} 1 & -\alpha^3 \\ 1 & 0 \end{vmatrix} = \alpha^3$
85.	$e(x) \cdot h(y) = (x + \alpha^2 y, \alpha^3 x + \alpha^3 y; 3, 6, 1)$	$\begin{vmatrix} 1 & \alpha^2 \\ \alpha^3 & \alpha^3 \end{vmatrix} = \alpha^3 + 1$
86.	$h(x) \cdot d^{-1}(y) = (x, \alpha x + \alpha^2 y; 3, 7, 1)$	$\begin{vmatrix} 1 & 0 \\ \alpha & \alpha^2 \end{vmatrix} = \alpha^2$
87.	$k(x) \cdot b(y) = (x + \alpha^4 y, \alpha x - \alpha y; 4, 1, 1)$	$\begin{vmatrix} 1 & \alpha^4 \\ \alpha & -\alpha \end{vmatrix} = 1 - \alpha$
88.	$h(x) \cdot c(y) = (x + \alpha^3 y, \alpha x + \alpha^2 y; 4, 2, 1)$	$\begin{vmatrix} 1 & \alpha^3 \\ \alpha & \alpha^2 \end{vmatrix} = \alpha^2 - \alpha^4$
89.	$f^{-1}(x) \cdot k(y) = (-\alpha^3 x + \alpha^4 y, \alpha^4 x - \alpha^4 y; 4, 3, 1)$	$\begin{vmatrix} -\alpha^3 & \alpha^4 \\ \alpha^4 & -\alpha^4 \end{vmatrix} = \alpha^3 - \alpha^2$
90.	$k^{-1}(x) \cdot g^{-1}(y) = (\alpha x - \alpha^4 y, \alpha^4 x; 4, 4, 1)$	$\begin{vmatrix} \alpha & -\alpha^4 \\ \alpha^4 & 0 \end{vmatrix} = -\alpha^3$
91.	$h(x) \cdot e(y) = (x + \alpha^3 y, \alpha x - y; 4, 5, 1)$	$\begin{vmatrix} 1 & \alpha^3 \\ \alpha & -1 \end{vmatrix} = -\alpha^4 - 1$
92.	$k(x) \cdot d^{-1}(y) = (x, \alpha x + \alpha y; 4, 6, 1)$	$\begin{vmatrix} 1 & 0 \\ \alpha & \alpha \end{vmatrix} = \alpha$
93.	$k(x) \cdot c(y) = (x + \alpha^4 y, \alpha x + \alpha y; 5, 1, 1)$	$\begin{vmatrix} 1 & \alpha^4 \\ \alpha & \alpha \end{vmatrix} = \alpha + 1$
94.	$f^{-1}(x) \cdot h(y) = (-\alpha^3 x + \alpha^4 y, \alpha^4 x - \alpha^4 y; 5, 2, 1)$	$\begin{vmatrix} -\alpha^3 & \alpha^4 \\ \alpha^4 & -\alpha^4 \end{vmatrix} = \alpha^3 - \alpha^2$
95.	$h^{-1}(x) \cdot g^{-1}(y) = (\alpha^2 x + y, \alpha^4 x; 5, 3, 1)$	$\begin{vmatrix} \alpha^2 & 1 \\ \alpha^4 & 0 \end{vmatrix} = -\alpha^4$
96.	$k(x) \cdot e(y) = (x + \alpha^4 y, \alpha x + \alpha^4 y; 5, 4, 1)$	$\begin{vmatrix} 1 & \alpha^4 \\ \alpha & \alpha^4 \end{vmatrix} = \alpha^4 + 1$
97.	$d(x) \cdot a(y) = (x - y, y; 5, 5, 1)$	$\begin{vmatrix} 1 & -1 \\ 0 & 1 \end{vmatrix} = 1$
98.	$h(x) \cdot f^{-1}(y) = (x + \alpha y, \alpha x - \alpha y; 6, 1, 1)$	$\begin{vmatrix} 1 & \alpha \\ \alpha & -\alpha \end{vmatrix} = -\alpha^2 - \alpha$
99.	$g^{-1}(x) \cdot h^{-1}(y) = (\alpha^3 x + \alpha^2 y, -\alpha^2 y; 6, 2, 1)$	$\begin{vmatrix} \alpha^3 & -\alpha^2 \\ 0 & -\alpha^2 \end{vmatrix} = 1$
100.	$a(x) \cdot e(y) = (x - y, x + \alpha^3 y; 6, 3, 1)$	$\begin{vmatrix} 1 & -1 \\ 1 & \alpha^3 \end{vmatrix} = \alpha^3 + 1$
101.	$d(x) \cdot k(y) = (x - \alpha y, y; 6, 4, 1)$	$\begin{vmatrix} 1 & -\alpha \\ 0 & 1 \end{vmatrix} = 1$
102.	$g^{-1}(x) \cdot k^{-1}(y) = (\alpha^3 x + \alpha^2 y, -\alpha y; 7, 1, 1)$	$\begin{vmatrix} \alpha^3 & \alpha^2 \\ 0 & -\alpha \end{vmatrix} = -\alpha^4$
103.	$k^{-1}(x) \cdot e(y) = (\alpha x - \alpha y, \alpha^4 x + \alpha^2 y; 7, 2, 1)$	$\begin{vmatrix} \alpha & -\alpha \\ \alpha^4 & \alpha^2 \end{vmatrix} = \alpha^3 + 1$
104.	$d(x) \cdot h(y) = (x - \alpha y, y; 7, 3, 1)$	$\begin{vmatrix} 1 & -\alpha \\ 0 & 1 \end{vmatrix} = 1$
105.	$h^{-1}(x) \cdot e(y) = (\alpha^2 x - \alpha^2 y, \alpha^4 x + \alpha y; 8, 1, 1)$	$\begin{vmatrix} \alpha^2 & -\alpha^2 \\ \alpha^4 & \alpha \end{vmatrix} = \alpha^3 + \alpha$
106.	$h(x) \cdot d(y) = (x + \alpha^3 y, \alpha x; 8, 2, 1)$	$\begin{vmatrix} 1 & \alpha^3 \\ \alpha & 0 \end{vmatrix} = -\alpha^4$
107.	$k(x) \cdot d(y) = (x + \alpha^4 y, \alpha x; 9, 1, 1)$	$\begin{vmatrix} 1 & \alpha^4 \\ \alpha & 0 \end{vmatrix} = 1$

Table 1: Products and determinants.

We can see that all the determinants are from the set  $\Lambda$  (Lemma 2), that is, coprime with  $n$ . For  $n = 1$  the group  $\Gamma$  consists of elements  $(0, 0; s)$ ,  $s \in \Delta_{10}$  and the corresponding Cayley graph  $G = \text{Cay}(\Delta_{10}, X)$  has diameter two, degree 16 and order 200, which gives  $|G| = 0.78125d^2$ .  $\square$

In the following lemma we use explicit estimates for the distribution of primes in arithmetic progressions to show that in a "short" interval there is always a prime  $p$  of the form  $p = 10s + 1$ . We will need the lemma in the proof of Main Theorem 2.

**Lemma 4.** *Let  $x$  be any real number  $x \geq 21221$ . Then there is a prime  $p$  of the form  $p = 10s + 1$  such that  $p \in (x; 1.0055856x)$ .*

*Proof.* We will prove the lemma separately for i)  $x \geq 10^{10}$ , ii)  $4.2 \cdot 10^6 \leq x \leq 10^{10}$  and iii)  $21221 \leq x \leq 4.2 \cdot 10^6$ . In the proof of i) and ii) we follow the paper [5] which is based on the work [12]. As usual, let  $\theta(x)$  denote the first Chebyshev function defined by  $\theta(x) = \sum_{p \leq x} \log p$ , where the sum is over all primes not exceeding  $x$ . If  $k$  and  $l$  are relatively prime and  $l \leq k$  the function  $\theta(x; k, l)$  is defined as

$$\theta(x; k, l) = \sum_{\substack{p \leq x \\ p \equiv l \pmod{k}}} \log p. \quad (1)$$

i) Let  $x \geq 10^{10}$ . Theorem [12, Theorem 1] says that for each positive real number  $x$  and for each coprime  $k, l$ ,  $l \leq k$ , there is an  $\epsilon = \epsilon(x, k)$  such that

$$\max_{1 \leq y \leq x} \left| \theta(y; k, l) - \frac{y}{\varphi(k)} \right| \leq \epsilon \frac{x}{\varphi(k)}. \quad (2)$$

The values of  $\epsilon$  for various quantities of  $x$  and  $k$  are given by [12, Table 1]. From the previous inequality it follows that

$$-\frac{\epsilon}{\varphi(k)}x \leq \theta(x; k, l) - \frac{x}{\varphi(k)} \leq \frac{\epsilon}{\varphi(k)}x. \quad (3)$$

Now let  $\delta \geq 0$ , let  $x' = (1 + \delta)x$  let  $\theta = \theta(x; k, l)$  and let  $\theta' = \theta(x'; k, l)$ . From (3) we have  $-\left(\theta - \frac{x}{\varphi(k)}\right) \geq -\frac{\epsilon}{\varphi(k)}x$  and  $\theta' - \frac{x'}{\varphi(k)} \geq -\frac{\epsilon}{\varphi(k)}x'$ . It follows that  $\theta' - \theta \geq \frac{x}{\varphi(k)}[(1 - \epsilon)(1 + \delta) - (1 + \epsilon)]$ . We see that if

$$(1 - \epsilon)(1 + \delta) - (1 + \epsilon) > 0 \quad (4)$$

then  $\theta' - \theta > 0$  and consequently the interval  $(x, x')$  contains a prime  $p \equiv l \pmod{k}$ . Solving the inequality (4) one can obtain  $\delta > \frac{2\epsilon}{1-\epsilon}$ . For  $k = 10$  and  $x \geq 10^{10}$  ([12, Table 1]) we have  $\epsilon = 0.002785$ . Since  $\frac{2 \cdot 0.002785}{1 - 0.002785} = 0.0055856$ , choosing  $\delta = 0.0055856$  we have: for  $x \geq 10^{10}$  there is a prime  $p \equiv 1 \pmod{10}$  in the interval  $(x, 1.0055856x)$ .

ii) Let  $4.2 \cdot 10^6 \leq x \leq 10^{10}$ . Theorem [12, Theorem 2] gives for each positive real number  $x \leq 10^{10}$  and for coprimes  $k, l$  and constant  $\gamma = \gamma(k)$  (given for various values of  $k$  by table [12, Table 2]) the inequality

$$\max_{1 \leq y \leq x} \left| \theta(y; k, l) - \frac{y}{\varphi(k)} \right| \leq \gamma \sqrt{x}. \quad (5)$$

From (5) we get inequalities  $-\left(\theta - \frac{x}{\varphi(k)}\right) \geq -\gamma \sqrt{x}$  and  $\theta' - \frac{x'}{\varphi(k)} \geq -\gamma \sqrt{x'}$ . It follows that  $\theta' - \theta \geq \sqrt{x} \left[ \frac{\delta}{\varphi(k)} \sqrt{x} - \gamma(1 + \sqrt{1 + \delta}) \right]$ . Solving the inequality

$$\frac{\delta}{\varphi(k)} \sqrt{x} - \gamma(1 + \sqrt{1 + \delta}) > 0 \quad (6)$$

we see that if  $x > \left[ \frac{\varphi(k)\gamma(\sqrt{1+\delta}+1)}{\delta} \right]^2$  then the interval  $(x, x') = (x, (1 + \delta)x)$  contains a prime  $p \equiv l \pmod{k}$  for each  $x \leq 10^{10}$ . For  $k = 10$  we have  $\varphi(k) = 4$  and (from the table [12, Table 2])  $\gamma(k) = 1.412480$ . Since  $\left[ \frac{4 \cdot 1.412480 \cdot (\sqrt{1+0.0055856}+1)}{0.0055856} \right]^2 = 4104075.014974$ , we have: for  $4.2 \cdot 10^6 \leq x \leq 10^{10}$  there is a prime  $p \equiv 1 \pmod{10}$  in the interval  $(x, 1.0055856x)$ .

iii) Let  $21221 \leq x \leq 4.2 \cdot 10^6$ . It is easy to check (e.g. by GAP) that the difference between every two consecutive primes  $21221 \leq p_1 = 10s_1 + 1 < p_2 = 10s_2 + 1 \leq 4.2 \cdot 10^6$  is always less than  $1.005p_1$ . That is, for  $21221 \leq x \leq 4.2 \cdot 10^6$  there is a prime  $p \equiv 1 \pmod{10}$  in the interval  $(x, 1.0055856x)$ .  $\square$

**Theorem 2** (Main Theorem).  $C(d, 2) > 0.684d^2$  for every integer  $d \geq 360756$ .

*Proof.* Let  $d = 17n - 1 + r$ ,  $r \in \{0, 1, \dots, 16\}$  (that is  $n \geq 20801$ ), let  $p$  be the greatest prime number of the form  $p = 10s + 1$  such that  $p \leq n$  and let  $d' = 17p - 1$ . By Theorem 1 there is a Cayley graph  $G'$  of diameter two, degree  $d'$  and of order  $\frac{200}{289}(d' + 1)^2$ . Adding  $d - d'$  additional generators to the generating set of the corresponding Cayley graph we obtain a Cayley graph  $G$  of degree  $d$  and of the same order as  $G'$ . By Lemma 4, for the number  $n$  we have  $p \leq n < (1 + \delta)p$  where  $\delta = 0.0055856$ . From the inequality  $n \leq (1 + \delta)p$  we get  $17n - 1 + r \leq (17p - 1) + 11\delta p + r$  that is  $d \leq d'(1 + \delta) + (\delta + r)$  and consequently  $d' + 1 \geq \frac{d+1-r}{1+\delta}$ . It follows that  $C(d, 2) = C(d', 2) = \frac{200}{289}(d' + 1)^2 \geq \frac{200}{289} \left( \frac{d+1-r}{1+\delta} \right)^2 \geq \frac{200}{289(1+\delta)^2} \left( 1 - \frac{15}{d} \right)^2 d^2$ . Since  $d \geq 360756$ , we have  $C(d, 2) \geq \frac{200}{289(1+\delta)^2} \left( 1 - \frac{15}{360756} \right)^2 d^2 \geq 0.684317d^2 > 0.684d^2$  for every integer  $d \geq 360756$ .  $\square$

#### 4. Conclusion and remarks

We have given a construction of Cayley graphs of diameter two with  $C(d, 2) \geq cd^2$  for every degree  $d$ , where  $c > 0$  is a positive constant. Let  $D$  be a degree, for which a Cayley graph constructed in [14] is defined. From the analysis in [1] it

follows, that in the interval  $(D; 2D)$  the construction with "c" gives better results for degrees  $d \in (\frac{1}{\sqrt{c}}D; 2D)$ . Let  $c' = \frac{1}{\sqrt{c}}$ . It follows that (roughly speaking) the ratio of number of better results for "c-construction" to the number of all constructions (up to a degree  $2^{s+1}D$ ) is given by  $\frac{(2D-c'D)+(4D-2c'D)+\dots+(2^{s+1}D-2^s c'D)}{2^{s+1}D}$  which has the limit  $2 - \frac{1}{\sqrt{c}}$  as  $D$  and  $s$  tend to infinity. On the other hand, if one counts the number of better results for "c-construction" in intervals  $(c'D; 2c'D)$ , the ratio is  $\frac{(2D-c'D)+(4D-2c'D)+\dots+(2^{s+1}D-2^s c'D)}{2^{s+1}c'D}$  which has the limit  $2\sqrt{c} - 1$ . It follows that the percentage of better results for "c-construction" is between  $2\sqrt{c} - 1$  and  $2 - \frac{1}{\sqrt{c}}$ . For  $c = \frac{200}{289}$  we have the interval  $(\frac{20\sqrt{2}}{11} - 1; 2 - \frac{17\sqrt{2}}{20})$  which is approximately  $(0.66378; 0.797918)$ . Below we can see the table of intervals of degrees (the computation was performed by GAP) for which our construction gives better results as the construction in [14]. In the second and third column of the table there is the ratio of the number of degrees when our construction gives better results as those in [14] to the number of all degrees for intervals  $(c'D; 2c'D)$  and  $(D; 2D)$ , respectively, for degrees  $D$  from  $10^3$  do  $10^{14}$ . We can see that these values approach the values  $\frac{20\sqrt{2}}{11} - 1 \approx 0.66378$  and  $2 - \frac{17\sqrt{2}}{20} \approx 0.797918$ , respectively.

Degrees for which our construction is better	Min ratio	Max ratio
$\langle 2566; 4345 \rangle$	0.702834	0.8
$\langle 4946; 8569 \rangle$	0.718946	0.828585
$\langle 9876; 16889 \rangle$	0.715155	0.835702
$\langle 19736; 33529 \rangle$	0.707326	0.832359
$\langle 39456; 66553 \rangle$	0.697199	0.826501
$\langle 78896; 132601 \rangle$	0.689772	0.819844
$\langle 157606; 264185 \rangle$	0.683042	0.814929
$\langle 315196; 527353 \rangle$	0.678087	0.810558
$\langle 630376; 1052665 \rangle$	0.674094	0.807227
$\langle 1260566; 2103289 \rangle$	0.671315	0.804675
$\langle 2521116; 4202489 \rangle$	0.669141	0.802819
$\langle 5042046; 8400889 \rangle$	0.667666	0.801425
$\langle 10083906; 16793593 \rangle$	0.666532	0.800446
$\langle 20167626; 33579001 \rangle$	0.665764	0.799718
$\langle 40335236; 67141625 \rangle$	0.665177	0.799208
$\langle 80670456; 134266873 \rangle$	0.664783	0.798831
$\langle 161340726; 268500985 \rangle$	0.664485	0.79857
$\langle 322681436; 536969209 \rangle$	0.664285	0.798378
$\langle 645362686; 1073872889 \rangle$	0.664134	0.798246
$\langle 1290725356; 2147680249 \rangle$	0.664034	0.798149
$\langle 2581450526; 4295229433 \rangle$	0.663958	0.798083
$\langle 5162900866; 8590327801 \rangle$	0.663907	0.798034
$\langle 10325801716; 17180393465 \rangle$	0.663869	0.798001

$\langle 20651603416; 34360524793 \rangle$	0.663844	0.797976
$\langle 41303206816; 68720525305 \rangle$	0.663825	0.79796
$\langle 82606413616; 137440526329 \rangle$	0.663812	0.797947
$\langle 165212827216; 274880004089 \rangle$	0.663803	0.797939
$\langle 330425654416; 549758959609 \rangle$	0.663797	0.797933
$\langle 660851308816; 1099515822073 \rangle$	0.663792	0.797929
$\langle 1321702617616; 2199029547001 \rangle$	0.663789	0.797926
$\langle 2643405235216; 4398054899705 \rangle$	0.663786	0.797924
$\langle 5286810470416; 8796105605113 \rangle$	0.663785	0.797922
$\langle 10573620940816; 17592202821625 \rangle$	0.663783	0.797921
$\langle 21147241881447; 35184397254649 \rangle$	0.663783	0.79792
$\langle 42294483762876; 70368777732089 \rangle$	0.663782	0.79792

Table 2: The numerical results for numbers of degrees when our construction is better as that in [14]

## Acknowledgements

I would like to express my gratitude to the referees for all the valuable and constructive comments.

The research was supported by VEGA Research Grant No. 1/0811/14 and by the Operational Programme 'Research & Development' funded by the European Regional Development Fund through implementation of the project ITMS 26220220179.

## References

- [1] M. Abas, *Cayley graphs of diameter two and any degree with order half of the Moore bound*, Discrete Applied Mathematics, **173**, (2014), 1–7
- [2] M. Abas, *On Record Cayley Graphs of Diameter Two*, Submitted for publication. Available as arXiv:1509.00842
- [3] W. G. Brown, *On graphs that do not contain a Thompsen graph*, Canad. Math. Bull., **9**, (1996), 281–285
- [4] P. J. Cameron, *Permutation groups*, Cambridge University Press, (1999)
- [5] J. Cullinan, F. Hajir, *Primes of prescribed congruence class in short intervals*, Integers, **12** (2012), Paper A56, 4 p., electronic only
- [6] R. M. Damerell, *On Moore graphs*, Proc. Cambridge Phil. Soc. **74**, (1973), 227–236.

- [7] P. Erdős, S. Fajtlowicz, A. J. Hoffman, *Maximum degree in graphs of diameter 2*, Networks, **10**, (1980), 87–90
- [8] A. J. Hoffman, R. R. Singleton, *On Moore graphs with diameter 2 and 3*, IBM J. Res. Develop. 4, (1960), 497–504.
- [9] M. Mačaj, J. Širáň, *Search for properties of the missing Moore graph*, Linear Algebra and its Applications, **432**, No. 9, (2010), 2381–398
- [10] B. D. McKay, M. Miller, J. Širáň, *A note on large graphs of diameter two and given maximum degree*, J. Combin. Theory Ser. B, **74**, (1998), 110–118
- [11] M. Miller, J. Širáň, *Moore graphs and beyond: a survey of the degree/diameter problem*, Electron. J. Combin. (2013) DS14
- [12] O. Ramaré, R. Rumely, *Primes in arithmetic progressions*, Mathematics of Computation, 65 (213), (1996), 397–425.
- [13] J. Šiagiová, J. Širáň, *A note on large Cayley graphs of diameter two and given degree*, Discrete Mathematics, **305**, No. 1-3, (2005), 379–382
- [14] J. Šiagiová, J. Širáň, *Approaching the Moore bound for diameter two by Cayley graphs*, Journal of Combinatorial Theory, Series B, **102**, No. 2, (2012), 470–473
- [15] J. Širáň, J. Šiagiová, M. Ždímalová, *Large graphs of diameter two and given degree*, In: Proc. IWONT 2010, Univ. Politcnica de Catalunya., 347–359.